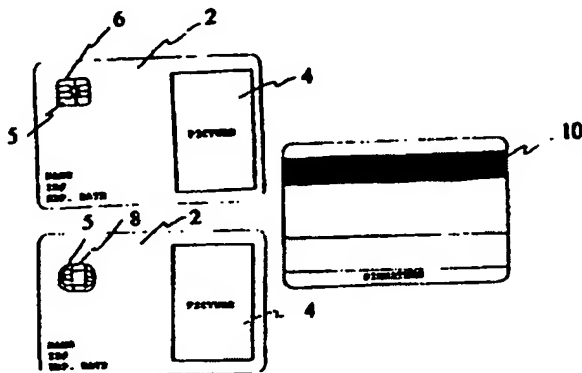




INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6: G07F 7/10, G06K 9/08		A2	(11) International Publication Number: WO 97/22092
			(43) International Publication Date: 19 June 1997 (19.06.97)
(21) International Application Number: PCT/US96/19418		(81) Designated States: BR, CA, CN, IL, JP, RU, TR, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).	
(22) International Filing Date: 13 December 1996 (13.12.96)			
(30) Priority Data: 08/572,751 14 December 1995 (14.12.95) US		Published Without international search report and to be republished upon receipt of that report.	
(71) Applicant: VENDA SECURITY CORPORATION [US/US]; 10 Blackburn Place, Palm Coast, FL 32137 (US).			
(72) Inventor: WOLF, Roland; 10 Blackburn Place, Palm Coast, FL 32137 (US).			
(74) Agents: WEIHROUCH, Steven, P. et al.; Oblon, Spivak, McClelland, Maier & Neustadt, P.C., Crystal Square Five, 4th floor, 1755 Jefferson Davis Highway, Arlington, VA 22202 (US).			

(54) Title: SECURE PERSONAL INFORMATION CARD AND METHOD OF USING THE SAME



(57) Abstract

A method and apparatus for storing general (or non confidential) and medical (or other confidential) information separately on a smart card to provide non-medical or unauthorized persons to access the general information while preventing access to the medical information. The method authenticates medical professionals using a medical professional smart card which includes an identification that the smart card belongs to a medical professional, and the method also authenticates an optional medical professional password before allowing access to the medical information stored on a smart card. Depending on the type of medical professional (or other authorized person) that is accessing the smart card, various levels of access are given to the card. For example, doctors are authorized to read and write medical history information and prescription information, while pharmacists are blocked from reading and writing medical history information and are further limited to reading and erasing prescription information without being able to write new prescription information. Similarly, emergency medical professionals can access a portion of the medical information needed to administer medical services (i.e., blood type and medical conditions). The general information is available to other service providers to ease in receiving services (e.g., reading name and address for immigration services, car and hotel rental).

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	GB	United Kingdom	MW	Malawi
AT	Austria	GE	Georgia	MX	Mexico
AU	Australia	GN	Guinea	NE	Niger
BB	Barbados	GR	Greece	NL	Netherlands
BE	Belgium	HU	Hungary	NO	Norway
BF	Burkina Faso	IE	Ireland	NZ	New Zealand
BG	Bulgaria	IT	Italy	PL	Poland
BJ	Benin	JP	Japan	PT	Portugal
BR	Brazil	KE	Kenya	RO	Romania
BY	Belarus	KG	Kyrgyzstan	RU	Russian Federation
CA	Canada	KP	Democratic People's Republic of Korea	SD	Sudan
CF	Central African Republic	KR	Republic of Korea	SE	Sweden
CG	Congo	KZ	Kazakhstan	SG	Singapore
CH	Switzerland	LJ	Liechtenstein	SI	Slovenia
CI	Côte d'Ivoire	LK	Sri Lanka	SK	Slovakia
CM	Cameroon	LR	Liberia	SN	Senegal
CN	China	LT	Lithuania	SZ	Swaziland
CS	Czechoslovakia	LU	Luxembourg	TD	Chad
CZ	Czech Republic	LV	Latvia	TG	Togo
DE	Germany	MC	Monaco	TJ	Tajikistan
DK	Denmark	MD	Republic of Moldova	TT	Trinidad and Tobago
EE	Estonia	MG	Madagascar	UA	Ukraine
ES	Spain	ML	Mali	UG	Uganda
FI	Finland	MN	Mongolia	US	United States of America
FR	France	MR	Mauritania	UZ	Uzbekistan
GA	Gabon			VN	Viet Nam

TITLE OF THE INVENTION

SECURE PERSONAL INFORMATION CARD
AND METHOD OF USING THE SAME

BACKGROUND OF THE INVENTIONField of the Invention:

This invention relates to the creation and use of a secure personal information card to store general information and to store medical information separately from the general information.

Description of the Background:

Currently, in order to provide medical history information (i.e., known allergies, blood type, current prescriptions, medical conditions) about a patient to doctors in several locations, patient information is centralized in a computer database to which doctors can request access, usually by telephone. This system is advantageous in its ability to allow doctors and emergency medical professionals to quickly access medical information concerning a patient with whom they are unfamiliar. However, because the access is by phone, the confidential patient information can be compromised by computer intruders, often known as hackers. Due to the importance and confidentiality of medical information, reliable but decentralized control of the information is needed.

-2-

Smart cards are currently being used in a series of applications throughout the United States and Europe. Smart cards are manufactured in various forms. For example, Bull of France manufactures the SCOT(xx) series of cards, including the SCOT 30, 60, 110 and 1000 cards. Gemplus also makes several series of microprocessor-based smart cards for GSM mobile communication systems (i.e., SIM2, SIM3, GemXplore 3K, GemXplore 8K), payment cards (i.e., PCOS, MPCOS16K, MPCOS24K, MPCOS64K) and multi-purpose cards (i.e., MCOS24K, MPCOS16K, MPCOS24K, MPCOS64K). Gemplus provides a software development kit to aid in the creation of applications using these microprocessor-based smart cards. Some microprocessor cards also optionally provide cryptographic schemes based on the Data Encryption Standard algorithm, DES, card customization to enable additional functionality to be added to the smart cards and a multi-purpose chip operating system. Details on DES and other encryption/decryption algorithms can be found in APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS AND SOURCE CODE IN C, by Bruce Schneier, and published by John Wiley & Sons, 1994, which is incorporated herein by reference. Additionally, Gemplus makes a series of memory-based products, including GEMPLUS Free-Access Memory Cards (GFM), GEMPLUS Protected Memory Cards (GPM) and GEMPLUS Authenticated Memory Cards (GAM).

In France, smart cards are used to provide a mechanism for purchasing telephone "units" consumed by telephone usage,

-3-

as would be available through the GPM cards. Furthermore, smart cards have been described, as in U.S. Patent 4,874,935 to Thomas L. Younger, wherein the smart card stores personalized information which can be read and written. Additionally, the connection, electrical, communication and other specifications for smart cards are set forth in International Standards Organizations' publications ISO 7816-1 through ISO 7816-5. The disclosures of Younger and ISO 7816-1 to ISO 7816-5 are incorporated herein by reference. Known systems such as Younger fail to provide a method for partitioning information on the smart card so that some information is available to all requestors while other information (e.g., medical history information) is available only to authorized users authenticated using a second smart card.

SUMMARY OF THE INVENTION

It is an object of the present invention to overcome the foregoing deficiencies.

It is another object of the present invention to provide a method of storing, on a smart card, general information separately from medical information.

It is a further object of the present invention to provide a method of authenticating that a medical professional (or other authorized person) is requesting access to medical information, and blocking access to the medical data if a

medical professional is not authenticated as requesting access to the medical information, while providing access to the medical information when a medical professional is authenticated.

It is another object of the present invention to provide a method for storing general information on a smart card in unencrypted form and storing medical information on the same smart card in encrypted form.

It is a further object of the present invention to provide a method for storing general information on a smart card in encrypted form using one key and storing medical information on the same smart card by encrypting the medical information with a key different than the key used to encrypt the general information.

It is yet another object of the present invention to provide a method for reading the general user information by non-medical personnel while blocking the reading of medical information.

It is a still further object of the present invention to allow reading of both general information and medical information by medical personnel.

It is yet another object of the present invention to provide limited types of access to medical information stored on a smart card by authenticating the type of medical professional requesting access to the card and providing either no access rights to the medical information, at least

one of read, write, update and clear rights for part of the medical information, or at least one of read, write, update and clear rights for all of the medical information.

It is a further object of the present invention to provide a method for visually and magnetically relating a person to information stored on a smart card by using a method of printing a user picture on a smart card, recording information on a magnetic strip on the smart card and encrypting medical information on the smart card differently than other general information stored on the smart card.

The above and additional objects and advantages are achieved according to the present invention which includes storing general information on a first smart card, storing medical information onto the first smart card separately from the general information, inserting the first smart card into a first smart card reader, inserting a second smart card into a second smart card reader, authenticating the second smart card inserted into the smart card reader as a medical personnel's smart card, and detecting whether a medical personnel's smart card was authenticated. Access to the medical information stored on the first smart card is blocked if a medical personnel's smart card is not authenticated as being inserted in the second smart card reader, while access is permitted to a portion of the medical data based on a type of inserted medical professional's smart card when a medical professional's smart card has been authenticated upon

insertion into a second smart card reader. Upon proper authentication, at least one of reading medical information, updating medical information and erasing medical information from the first smart card are permitted using the provided access.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete appreciation of the invention and many of the attendant advantages thereof will be readily obtained as the same becomes better understood by reference to the following detailed description, when considered in connection with the accompanying drawings, wherein:

Figure 1A is a schematic of one embodiment of a smart card utilized according to the present invention;

Figure 1B is a schematic of a second embodiment of a smart card utilized according to the present invention;

Figure 1C is a schematic showing the reverse side of a smart card according to the first and second embodiments of smart cards to be used according to the present invention;

Figure 2 is a schematic of a computer system attached to a smart card reader, with the computer system performing a method of the present invention;

Figure 3 is a schematic of a screen for inputting the personal information to be stored on a smart card according to the present invention;

Figure 4 is a flowchart showing a general method of programming and using a smart card according to the present invention;

Figure 5 is a schematic of a screen for inputting the medical information according to the present invention;

Figure 6A is a schematic of a first access rights table to determine the type of access that is allowed to a first smart card based on a supplied PIN;

Figure 6B is a schematic of a second access rights table to determine the type of access that is allowed to a first smart card based on a supplied PIN;

Figure 6C is a schematic of a third access rights table to determine the type of access that is allowed to a first smart card based on a supplied PIN;

Figure 7 is a flowchart depicting a method of programming and using a smart card according to another embodiment of the present invention;

Figure 8 is a schematic of a screen for inputting immigration information according to the present invention;

Figure 9 is a schematic of a screen for inputting hotel register information according to the present invention;

Figure 10 is a schematic of a screen for inputting car rental information according to the present invention;

Figure 11A is a flowchart depicting three types of access allowed to the smart card;

Figure 11B is a flowchart showing five additional types of access allowed to the smart card of the present invention; and

Figure 12 is a schematic showing a telephone adapted to receive a smart card with a magnetic strip.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring now to the drawings, wherein like reference numerals designate identical or corresponding parts throughout the several views, Figure 1A is a view showing a first embodiment of a smart card 2 utilized according to the present invention. Smart card 2 includes a picture 4 and a smart card chip 8, with the smart card chip 8 containing plural leads 5. A second embodiment of a smart card 2 is shown in Figure 1B, in which picture 4 is also available and a different smart card chip 6 is present on the front face of the smart card 2, again with plural leads 5. The position of the leads is set forth in ISO 7186-2. In both the smart card of Figures 1A and 1B, a magnetic strip 10 is attached to the back face of the smart card 2. The smart card can therefore be used for identification as well as information storage. For example, the smart card can be used to prove identity when making credit card purchases. The picture 4 is used in combination with information stored on the magnetic strip or smart card chip about what credit cards a person is authorized to use. Furthermore, in a preferred embodiment, the picture 4 is

-9-

printed directly onto the smart cards to prevent someone from removing a laminated picture, adding a new picture in the place of the original picture and relaminating the smart card. In order to protect customers from fraudulent use of their credit cards, parts of customers' credit card numbers are stored on the smart card or magnetic strip. For example, in the case of a customer with a credit card number "123-456-789-0," on the smart card would be stored "235689" which is a portion of the whole number. When purchases are made, retailers could automatically cross-check credit cards with smart cards by reading the partial number from the smart card or magnetic strip, then swiping the credit card as normally occurs. If the credit card number does not match one of the partial numbers on the smart card, authorization is automatically denied, thereby protecting against unauthorized use. Furthermore, by only storing a portion of the credit card number on the smart card, the full credit card number is not compromised if the smart card is lost.

In general, the smart card 2 is used in conjunction with a computer system 20 which is attached to a double smart card reader 38 or a pair of single smart card readers 39. Computer system 20 comprises a motherboard 22, a central processing unit 24 (i.e., Intel 80x86, Motorola 680x0, PowerPC, Sparc, DEC Alpha), and memory 26. The computer system further includes programs on a high capacity fixed storage device (i.e., SCSI or IDE devices) 28 for manipulating the smart

cards. Additional removable storage media devices 30 provide a means for updating the programs stored on the high capacity fixed storage device 28 and the smart card 2. Further, a network adaptor 31 provides another means for updating programs and the smart card 2. The monitor 32 provides a method for interactively updating the information stored on a smart card, while input devices (keyboard 34 and mouse 36) provide a means for entering data to be stored on the smart card 2. The smart card 2 is read by either a double smart card reader 38 or by plural single smart card readers 39. A generic smart card reader, GCR500, is available from Gemplus and can be used to read and write data stored on a smart card 2. Bull also makes a smart card reader/writer unit named the CP8. In addition, the magnetic strip on the back of the smart card can be read by a magnetic strip reader 37. It is also possible for either of the smart card readers (38 and 39) to be equipped with a magnetic strip reader to provide a combined magnetic strip and smart card reader. These smart card readers (38 and 39) can also be housed in the computer system 20.

The programs stored on high capacity fixed storage device 28 include a series of programs which allow data to be read from or written to the smart card 2 according to the types of accesses allowed by the reader or writer. In addition to information to be stored to the smart card according to the present invention, data is also written at the manufacturing

stage and at a customization phase. During these phases, a unique ID for the card, a manufacturer's ID, a manufacturing date and other information is stored permanently and may not be modified.

Figure 3 shows part of a representative set of information 40 to be stored on a smart card 2 by the present invention. This information 40 is split into several segments, with access to individual segments being controlled by the rights of the requestor. The personality information 41 contains the general information about the owner of a smart card and is written to a blank smart card 2 during a customization process. A user's family name, first name, address, country of citizenship, country of residence, birthdate, language, place of birth, social security number, height and sex are all permanently associated with the card during the customization process. A card owner's phone number, driver's license number, issuing country, license expiration date, auto insurance carrier, policy number, profession, emergency contact, second emergency contact, religion and city in which his/her visa was issued are shown as representative of the type of information that can be generally stored about a user which may change and therefore may need to be updated.

Medical information 42 includes more specific information about a card's owner which is independently protected from other personal information 41. The medical information

-12-

includes, but is not limited to, an attending doctor's name, phone numbers (both office and emergency), fax number, time zone and, native language, along with a person's medical insurance information (i.e., policy number and co-insurance company). The information about a user's attending physician can be used to contact the attending physician in case of an emergency. The information allows the physician to be automatically dialed by emergency medical professionals or other medical professionals to receive additional information about a patient in need of care. By storing both a phone number for use during normal office hours and an emergency or pager number, a patient's attending physician can always be contacted. In an automatic dialing system using the smart card 2, the emergency/pager number is automatically dialed after receiving no answer at the office number. The caller and the attending physician may also be directly connected by computer where the computer system of the caller and the computer system of the attending physician are connected by the automatic dialing system. By connecting the computers, additional information (including a more extensive medical history, x-rays, test results, etc.) can quickly be transferred to the caller.

Medical information 46 may be stored as either text or as medical codes/numbers designating, e.g., symptoms or diagnoses describing a patient's condition. By using a medical code system, more information can be stored on the same card. By

-13-

medical codes, it should be understood that numbers, letters or a mixture can be used to represent a standardized condition. For example, "H1" is used to represent a failing heart valve, "H2" is use to represent the presence of a pace maker, "A1" is used to represent an allergy to penicillin, etc.

Furthermore, business, airline and service provider (hotel, car, immigration) information 43 can be stored as an addition to the updatable part of the general information 41.

Medical and general information is also stored on a second smart card 2, belonging to a medical professional. According to the type of medical professional whose card is being programmed, in addition to the general and medical information of the medical professional, a means for identifying the type of smart card is also stored on the smart card 2 of the medical professional. Optionally, a medical professional password is also stored on the smart card 2 of the medical professional.

After the information of Figure 3 is initially programmed onto a smart card in the respective information positions with their respective security, the information may be needed and recalled in various medical (i.e., during doctor visits, or in emergency medical situations) and non-medical (i.e., immigration, hotel registration, car rental) situations. For simplicity, the examples given below will be described using a user's/patient's smart card in a first smart card reader 39

-14-

and a doctor's smart card in a second smart card reader 39, although the method works equally well with the user's/patient's smart card being inserted into a first slot in a double smart card reader 38 and the doctor's smart card being inserted into a second slot of the double smart card reader 38.

As shown in Figure 4, a doctor uses a computer system to access medical information 46, by inserting a patient's smart card into a first of two smart card readers 39. The doctor's smart card 2 then is inserted into a second smart card reader 39. Having detected the presence of a smart card 2 in the second smart card reader, the computer system controlling access to the general and medical information starts the first step in allowing access to the medical information 46. The computer system determines whether the card inserted into the second smart card reader is a doctor's card. If the card inserted into the second smart card reader is not a doctor's card, appropriate failure processing is performed by the computer system (i.e., an error message is displayed, or audible alarm is emitted), and access to the medical information 46 is not provided by the computer system.

As an optional security measure, a second step to allowing access to the medical information 46 of a patient is performed by reading a password from the keyboard 34 to ensure that a doctor's lost smart card 2 cannot be used to read medical information 46 by un-authorized individuals. The

-15-

password is authenticated by the computer system, and if the password authentication is unsuccessful, the computer system performs appropriate failure processing. If the password is authenticated, the computer system provides read and write access to the medical information 46. The medical information 46 is then read or written as required by the doctor. As shown in Figure 5, the medical information 46 is used to check blood types, existing conditions, medical history, etc., and the computer system updates the medical information 46, including prescription information, as requested by the doctor. In an embodiment where medical conditions are stored using a coded form rather than text, the computer system is also equipped with a means for decoding the diagnosis or symptom codes and displaying information about the condition which the code represents. This means for decoding includes at least one of a textual description, an audible description and a visual description, wherein the visual description is represented with an animated or virtual body.

Furthermore, in another embodiment of the computer system of the present invention, the prompts (used to display or receive general information and medical information from the smart card and provided to a computer display 32) are in a native language of choice, either according to who is using the display or according to the language specified by an authenticating card.

In the first embodiment, a non-volatile memory card is used to implement doctor and user/patient smart cards. Because these smart cards provide no automatic protection, the segmentation and protection of the medical information 46 from the general information is done by the computer system. First, general and medical information are written to plural smart cards to be used in the computer system, along with an indication of whether or not each card being programmed is for a doctor or other special function person and, if so, a password or Personal Identification Number (PIN) corresponding to the card is also optionally written. Next, first and second programmed smart cards are inserted into first and second smart card readers. If the second smart card is determined to be a doctor's card, then the password or PIN is optionally prompted to further authenticate that the person using the second smart card is authorized to do so. Having authenticated the doctor, the computer system controls the reading of information from the first smart card and the writing of medical information back to the first smart card to correspond to the information entered into the computer system using a computer entry screen comparable to Figure 5.

In an alternate embodiment of the present invention, the overall security of the medical information is increased by encrypting the medical information using an encryption algorithm, preferably a symmetric algorithm (i.e., DES), and a shared key, i.e., shared by medical professionals. Before the

-17-

computer system provides access to the medical information, the shared key is read from an authenticated smart card 2 of a medical professional. The computer system then would decrypt the medical data using the shared key before displaying the data on the computer screen, and before writing medical information to the first smart card, the computer system encrypts the data entered on the computer screen by using the shared key.

In yet another embodiment of the present invention, which uses memory cards as smart cards, the doctor's password is required and is stored on the doctor's smart card in encrypted form. To prevent unauthorized reading of the shared key, the shared key is encrypted using the doctor's password. The computer system can still authenticate the doctor's password by encrypting the password typed by the doctor and comparing it with the encrypted version stored on the smart card. The typed password is then used to decrypt the shared key, preventing the shared key from being compromised by reading from a doctor's lost memory-based smart card. In this embodiment, when a doctor changes his password, both the stored, encrypted password and the encrypted shared key must be updated.

In a further embodiment of the present invention, which uses memory cards as smart cards, the doctor's password is required and stored on the smart card in encrypted form and the means for indicating that the smart card is a doctor's

card and shared key are encrypted using the plain text version of the doctor's password, then stored on the smart card.

In another embodiment of the present invention in which a microprocessor-based smart card is used, a smart card is programmed with medical information 46 stored in one area of the smart card containing one set of access rights, and the general information is stored in a separate area of the smart card with a different set of access rights. Furthermore, an indication of the type (i.e., doctor's, pharmacist's, emergency professional's) of the smart card is stored in an area that either cannot be directly read or cannot be modified. The smart card controls enforcing the rights to the information.

When a second smart card is inserted into the second smart card reader, the computer system sends a command to authenticate that the second smart card is a doctor card. If the second smart card determines that it is not a doctor's card, appropriate error processing is performed. If the second smart card determines that it is a doctor's card, then the computer system waits for the doctor to type a password. This password is sent to the second smart card to authenticate that it matches the internally stored password. If the password is authenticated, then a protected area in the second smart card is made readable and a PIN is read from the protected area of the second smart card. This PIN is written

to the first smart card to allow read and write access to the medical information.

In the case of a password mismatch, the second smart card can be used to monitor the number of password mismatches to see if a doctor's password is being guessed at or "hacked." By having set at customization a maximum number of allowable mismatches, the second smart card can disable itself when the maximum number of wrong guesses occurs. This provides a definite advantage over storing an encrypted password on a memory card. The encrypted password could be read by a hacker, and attacked by using several known techniques (i.e., dictionary attack, brute force, random guessing) until a guessed password matches the encrypted password stored on the card. The password, having been compromised, could then be used to determine the key or PIN used to access the medical information stored on the first smart card.

In a further embodiment of the present invention using microprocessor smart cards, as shown in Figure 7, the process of encrypting medical information to be stored on the first smart card and decrypting medical information read from the first smart card is performed internally in the second smart card. The second smart card is first authenticated as described above, medical data is then read from the first card in blocks and sent to the second smart card, and the second smart card sends back the decrypted medical data. The process is performed in reverse when storing information back to the

-20-

first smart card. Information to be encrypted is sent in blocks from the computer system to the second smart card, encrypted, read out of the second smart card and written back to the first smart card.

Obviously, a computer system could support any of the above embodiments or a combination of embodiments where the computer system automatically determines the type of each smart card and the processing required to authenticate the doctor's card and read and write the user's card. However, a presently preferred embodiment utilizes microprocessor based smart cards with multiple protectable areas with multiple sets of access rights or areas.

As shown in Figures 6A-6C, the access rights for separate areas can be established in several ways. In the figures, access permissions are given by "R" for read, "W" for write, "C" for clear and "D" for decrement, as in refill numbers for prescription information. For PIN columns with an entry indicated by "0", no PIN is required for the shown type of access. Figure 6A shows that a fixed number of entries are used to define rights for a single area per entry based on PINs. Using this configuration, access permissions may be distributed according to what PINs need access to what areas without presetting a number of PINs that can be assigned to any given area. Any PIN not in the list only allows access to the areas with a "0" PIN, and any PIN not associated with all areas only allows access to the areas with a "0" PIN and the

-21-

areas for which a matching PIN exists. However, this requires storing an additional piece of information per entry, i.e., the area identifier.

Figure 6B depicts an arrangement which avoids the need to store an area identifier per entry, by fixing the number of PINs per area and a search for valid PINs for a given area can be performed by knowing the number of PINs per area. However, this configuration is more restrictive than the configuration of Figure 6A. For area 1, only one entry is needed because read access is always provided and no other rights are assigned to area 1. Therefore, all other associated entries for area 1 are wasted.

A third configuration combines 6A and 6B and uses a map of all areas and the access rights allowed to each area based on the PINs specified in the first column. This configuration is advantageous in cases where different rights for many different areas are assigned to each PIN.

As an illustrative example of how these access controls can be utilized, the division of information the smart card will be referenced with respect to Figures 6A-6C. The first area, area 1, is used as the general information area and is assigned with a PIN number "0" which represents that all users have the access rights shown for area 1. As the rights for area 1 are indicated by an "R", area 1 only may be read by all users. However, area 2 is used as the area in which medical information is stored, and access to this area is restricted

-22-

until after authenticating a doctor. This PIN code, "1234," is then read from a protected area of the second smart card and the PIN is then written to the patient's smart card, unlocking area 2. Because the PIN "1234" provides read, write and clear access, an authenticated doctor can perform any of these operations on the medical data. As shown in Figure 6B, area 1 has a single PIN of "0" allowing read access by all users. Further below, PIN "1234" is provided in area 1 and allows read, write and clear access by a doctor. As shown in Figure 6C, PIN "0" allows read access to all users for area 1, while PIN "1234" allows read access to area 1 and read, write and clear access for area 2.

In each of the above embodiments, access rights have been used to partition the general information from the medical information based on whether a smart card had doctor's rights. An additional level of rights is added in another embodiment of the present invention wherein a pharmacist is given read access, but not write access, to the prescription portion of the medical information so that the pharmacist can fill prescriptions written by a doctor that are stored on a smart card. However, in this embodiment, the pharmacist is blocked from reading or writing the rest of the medical information. In an embodiment using no encryption on a memory-based smart card, the computer system enforces the protection by only reading and displaying prescription information from the

-23-

medical information and not allowing writing to the prescription information.

In a memory-based smart card embodiment where encryption is used, the computer system encrypts the prescription portion of the medical information shared by pharmacists and doctors, and encrypts the rest of the medical information using a shared key for doctors that is not known to pharmacists. Furthermore, all the methods used to encrypt means for identifying doctor cards and doctor passwords are also applicable to encrypting the means for identifying pharmacist cards and passwords.

Additionally, the pharmacist's rights may also include the right to decrement the number of refills to which a patient is entitled. In both the method that uses no encryption and the method that uses encryption, because the computer system must be able to write/update the prescription information, the computer system restricts the number of refills of a drug is only decremented and not incremented or set to a new value. For added protection, in yet another alternate embodiment, all prescriptions written by doctors are electronically "signed" using an encryption algorithm, preferably a public key encryption algorithm, and the electronic "signature" is authorized before a prescription is filled.

In a preferred embodiment of the present invention, processor-based smart cards are used to provide access control

-24-

to the various types of information on the smart card. According to Figures 6A-6C, general information is stored in area 1, prescription information is stored in area 3 and all non-prescription medical information is stored in area 2. By using PIN "5678," the smart card controls enforcement of rights to the information, for example, such that pharmacists are given read, clear and decrement access to the prescription information without being given any permission for the rest of the medical information. When a second smart card is inserted into the second smart card reader, the computer system sends a command to authenticate that the second smart card is a pharmacist card. If the second smart card determines that it is not a pharmacist's card, appropriate error processing is performed. If the second smart card determines that it is a pharmacist's card, then the computer system waits for the pharmacist to type a password. This password is sent to the second smart card to authenticate that it matches the internally stored password. If the password is authenticated, then a protected area in the second smart card is made readable and a PIN is read from the protected area of the second smart card. This PIN is written to the first smart card to allow read access to the prescription information without providing write access to the prescription information and without providing read or write access to the rest of the medical information.

-25-

This access control is made possible by storing the prescription information in an area (area 3) separately protected from the rest of the medical information, which is in area 2. The first smart card allows direct read and write access to the prescription information and medical information when a doctor's PIN is read from the second smart card and written to the first smart card, but only allows direct read access to the prescription information and no access to the rest of the medical information area when a pharmacist's PIN is read from the second smart card and written to the first smart card. Additionally, erase and decrement functions for prescription information on the first smart card are performed by sending either the doctor's or the pharmacist's PIN to the first smart card, and then sending a command to erase prescription information or decrement the number of available refills. Since the microprocessor in the first smart card performs these functions, unauthorized writing or refilling of prescription information is prevented.

Because the blood type, medical alert and medication information is also often required by emergency personnel, a portion of medical information 46 is available by using an emergency service's smart card. Providing access to part, but not all, of the medical information is provided by methods analogous to providing access to prescription information by pharmacists without providing access to all medical information. In this embodiment of the present invention,

-26-

general information is stored in area 1, prescription information is stored in area 3 and medical information required by emergency personnel is stored in area 4. All remaining medical information is stored in area 2 and the access rights in Figure 6A-6B are assigned to the areas. Again, a doctor's card uses PIN "1234," a pharmacist's card uses PIN "5678" and medical emergency personnel's card uses PIN "0911." This provides a doctor with read and write access to all medical information areas while allowing a pharmacist read, clear and decrement privileges for the prescription information but no further access rights to any other parts of the medical information. Emergency medical professionals' cards use PIN "0911" and are allowed read access to the prescription information in area 3 and the medical alert information in area 4. Availability of this information is very helpful in cases where an accident victim is unconscious or does not have an adequate command of the language used by the emergency medical professionals.

The segmented general and medical information is also used in alternate embodiments of the present invention to aid in providing parts of the general information to police, insurance and other service providers, banks, immigrations and customs, hotel, automotive, etc., while protecting service specific information from other unauthorized service providers. Figure 8 shows a computer screen utilizing a portion of using parts of the general information 41, wherein

-27-

th general information is used in completing an immigration application. Immigration information 49 contains a subset of the general information 41 stored on the smart card 2. Furthermore, the immigration access optionally allows the address 50 in the visited country (e.g., United States) and the information for immigration 51 (i.e., date of departure) to be read and updated by authorized immigration personnel. Although not shown, visa type is also recordable on the smart card, for example, to reflect the length of stay allowed in a country being visited. At departure, the date and time of arrival can be read from the smart card to automatically generate an embarkment card or any other immigration papers required upon entering/exiting a country. Furthermore, the identity of the departing individual can be recorded and uploaded to an immigration computer or a central immigration computer to track visitors to the country. Additionally, using a double key system, as was used for pharmacists, doctors, etc., every entry and exit to a country can be recorded on the smart card.

Figure 9 shows a computer screen associated with using portions of the general information 41 to speed the registration process at a hotel. By reading parts of the general information 41, while blocking reading of the medical information 42, a hotel can more accurately register guests. However, a user may optionally erase its own hotel information using a PIN before checking into a new hotel to prevent one

hotel from learning other hotels at which the user stays. Part of this hotel information may likewise be read by taxis and other professional drivers to enable people with a poor command of a language to indicate where they wish to be taken. Taxis would be prevented from reading the hotel room number, although they would be given the street address of the hotel and optionally directions to the hotel. This same information is available to police and emergency professionals in order to be able to contact other members of a user's family in case of an accident.

A similar process can be performed for other service industries, such as car rentals shown in Figure 10, by reading a portion of the general information 41 from the smart card and applying it to a car rental registration template 56.

Figures 11A and 11B show an overall set of representative types of information to be stored on a smart card, the type of professional that is allowed access to each type of information, and what types of access to the available types of information each professional is permitted.

Figure 12 shows another use of the combination smart card and magnetic card of the present invention. Because this card is envisioned to be used by people who do not possess a strong command of a language of the country in which they are visiting, a combination phone and smart card/magnetic strip combines the information stored on the magnetic strip/smart card with automatic dialing and caller identification.

Emergency medical professionals can therefore be dispatched directly to a telephone used to call in an emergency, and the professionals dispatched are sent based on the information read from the card (i.e., based on language, age, medical condition of the owner of the smart card).

Obviously, numerous modifications and variations of the present invention are possible in light of the above teachings. It is therefore to be understood that within the scope of the appended claims, the invention may be practiced otherwise than as specifically described herein.

CLAIMS:

1. A method for restricting access to information stored on a first smart card by verifying authorization to access the information using a second smart card, comprising the steps of:

inserting a first smart card into a first smart card reader, the first smart card comprising first and second information areas, wherein access to the second information area is restricted;

inserting a second smart card into a second smart card reader, the second smart card comprising a means readable by the second smart card reader for determining a type of the second smart card;

reading the type of the second smart card using the second smart card reader;

verifying that the second smart card is authorized to access the second information area of the first smart card;

blocking access to the second information area of the first smart card if the verifying step indicates that the second smart card is not authorized to access the second information area of the first smart card; and

providing access to the second information area of the first smart card if the verifying step indicates that the

second smart card is authorized to access the second information area of the first smart card.

2. The method according to Claim 1, further comprising:
programming the first smart card with general information in the first information area and medical information in the second information area; and

programming the second smart card with the type of the second smart card.

3. The method according to Claim 2, wherein the step of programming the first smart card comprises:

programming the first information area of a memory-based smart card with general information in unencrypted form; and

programming the second information area with medical information in encrypted form.

4. The method according to Claim 3, wherein the step of programming the second information area in encrypted form comprises:

programming the second information area with medical information encrypted using DES.

5. The method according to Claim 4, comprising the step of:

programming the second smart card with DES key used to encrypt the medical information on the first smart card.

6. The method according to Claim 2, wherein the step of programming the first smart card comprises:

-32-

programming a microprocessor-based smart card with general information in the first information area;

assigning access rights to the first information area so that the first information area is read-only at all times;

programming the second information area with medical information; and

assigning access rights to the second information area so that a PIN is required to be sent to the first smart card to access information stored in the second information area of the first smart card.

7. The method according to Claim 2, further comprising: programming the second smart card with a password to authenticate use of the second smart card.

8. The method according to the Claim 7, wherein the step of programming a password comprises:

programming the second smart card with an encrypted password.

9. The method according to Claim 7, wherein the step of verifying that the second smart card is authorized to access the second information area comprises:

comparing the type of the second smart card read using the second smart card reader with a stored type of smart card which is authorized to access the second information of the first smart card;

denying access to the second information area of the first smart card if the comparing step indicates that the type

read from the second smart card reader and the known type are equal;

reading a password from a keyboard;

comparing the password read from the keyboard with the password stored on the second smart card; and

indicating that the second smart card is not authorized to access the second information of the first smart card when the passwords are not equal.

10. The method according to Claim 8, wherein the step of verifying that the second smart card is authorized to access the second information area comprises:

comparing the type of the second smart card read using the second smart card reader with a stored type of smart card which is authorized to access the second information of the first smart card;

denying access to the second information area of the first smart card if the comparing step indicates that the type read from the second smart card reader and the known type are equal;

reading a password from a keyboard;

comparing the password read from the keyboard with the password stored on the second smart card; and

indicating that the second smart card is not authorized to access the second information of the first smart card when the passwords are not equal.

11. The method according to Claim 8, wherein the step of comparing the password read from the keyboard comprises:

encrypting the password read from the keyboard to generate an encrypted keyboard password; and

comparing the encrypted keyboard password with the encrypted password stored on the second smart card.

12. The method according to Claim 2, wherein the step of programming the first smart card with medical information in the second information area comprises:

programming the medical information using medical codes.

13. A computer-implemented method of authorizing the use of a credit card based on information stored on a smart card containing a magnetic strip, comprising the steps of:

storing a portion of a credit card number to a smart card;

reading using a sales terminal the portion of the credit card number stored to the smart card;

reading a full credit card number from a magnetic strip on a credit card;

comparing the full credit card number to the portion of the credit card number stored to the smart card;

denying the use of the credit card if the comparing step indicates that the numbers are not related; and

authorizing the use of the credit card if the comparing step indicates that the numbers are related.

14. A computer-implemented method of contacting emergency professionals by phone, comprising the steps of:
- inserting a smart card with a magnetic strip into a reader in a telephone;
 - reading information stored on the smart card using the reader;
 - dialing emergency professionals automatically using the telephone;
 - transmitting the information read from the smart card using the reader from the telephone to a central dispatch unit; and
 - dispatching emergency professionals based on the information transmitted to the central dispatch unit.
15. The method according to Claim 12,
- wherein the step of transmitting the information read from the smart card comprises transmitting a native language of an owner of the smart card; and
 - wherein the step of dispatching emergency professionals comprises dispatching origins of professionals based on the native language transmitted in the transmitting step.
16. The method according to Claim 12, wherein the step of reading information stored on the smart card using the reader comprises:
- reading information stored on a chip on the smart card using a smart card reader.

17. The method according to Claim 12, wherein the step of reading information stored on the smart card using the reader comprises:

reading information stored on the magnetic strip of the smart card using a magnetic strip reader.

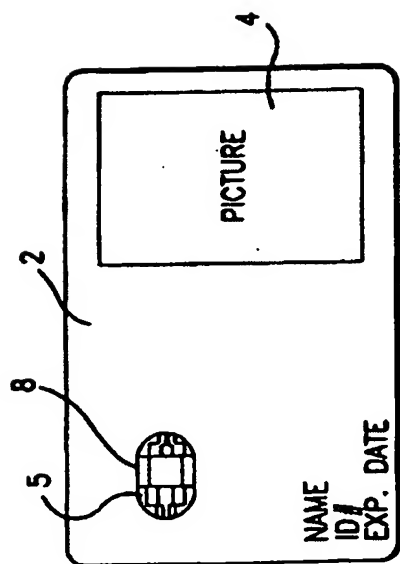


FIG. 1A

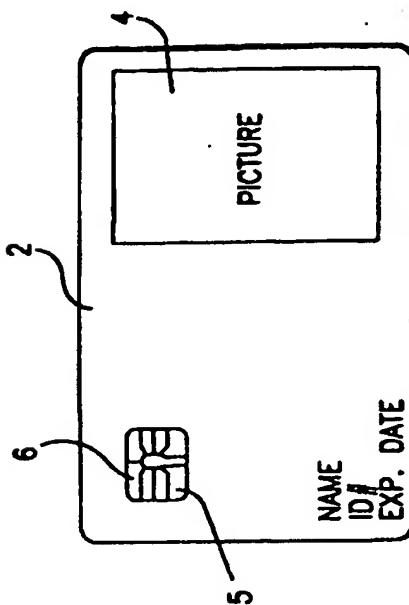


FIG. 1B

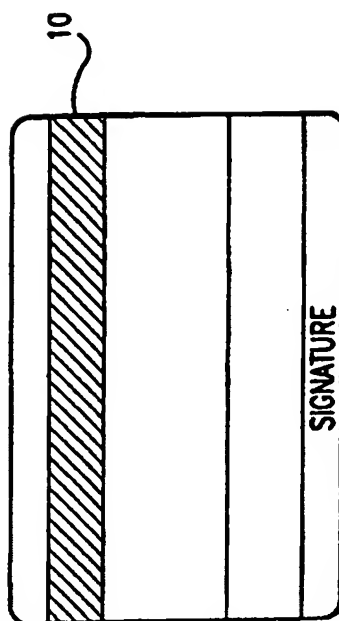


FIG. 1C

2/15

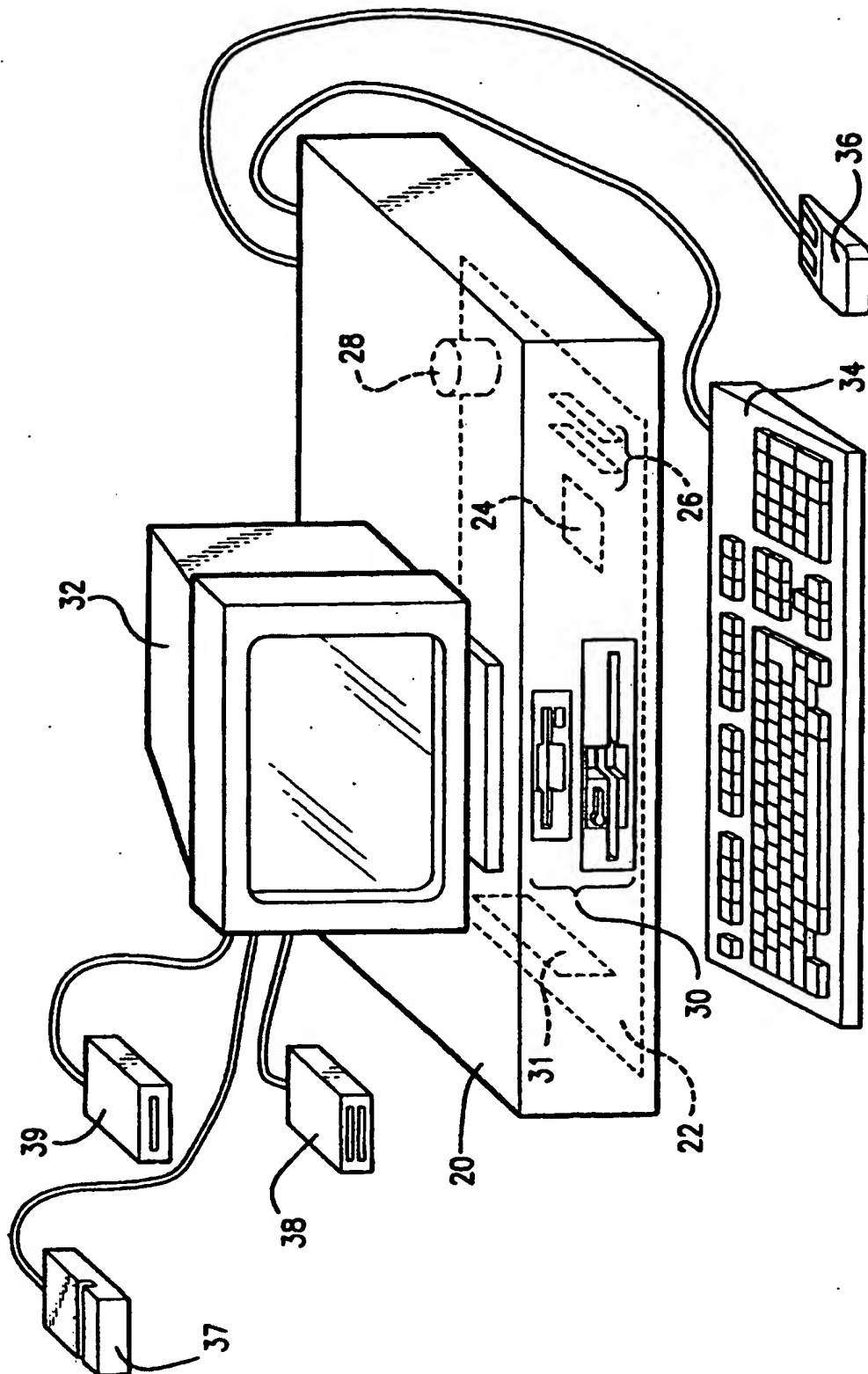


FIG. 2

3/15

ALL INFORMATION OF PERSONALITY			
DATE ISSUED	07.10.1995	CARD EXPIRATION DATE	07.10.1996
PERSONALITIES			
ID# (PASSPORT#)	<input type="text"/>	PHONE# WITH COUNTRY CODE	<input type="text"/>
FAMILY NAME	<input type="text"/>	DRIVER'S LICENSE	<input type="text"/>
FIRST NAME	<input type="text"/>	COUNTRY ISSUED	<input type="text"/>
ADDRESS	<input type="text"/>	LICENCE EXPIRATION DATE	<input type="text"/>
CITY, STATE	<input type="text"/>	AUTO INSURANCE CARRIER	<input type="text"/>
ZIP CODE	<input type="text"/>	POLICY NUMBER	<input type="text"/>
COUNTRY OF CITIZENSHIP	<input type="text"/>	PROFESSION	<input type="text"/>
COUNTRY OF RESIDENCE	<input type="text"/>	EMERGENCY CONTACT	<input type="text"/>
BIRTH DATE	<input type="text"/>	SECOND CONTACT	<input type="text"/>
LANGUAGE	<input type="text"/>	RELIGION	<input type="text"/>
PLACE OF BIRTH	<input type="text"/>	CITY-VISA ISSUED	<input type="text"/>
	<input type="text"/>	HEIGHT <input type="text"/>	SEX <input type="text"/>
MEDICAL INFORMATION			
DOCTOR'S NAME	<input type="text"/>	LANGUAGE	<input type="text"/>
PHONE# (W/COUNTRY CODE)	<input type="text"/>	MEDICAL INSURANCE COMPANY	<input type="text"/>
FAX# (W/COUNTRY CODE)	<input type="text"/>	POLICY NUMBER	<input type="text"/>
TIME ZONE	<input type="text"/>	CO-INSURANCE COMPANY	<input type="text"/>
BUSINESS/AIRLINE INFORMATION			
COMPANY CODE	<input type="text"/>	NUMBER OF VISITS PER YEAR	<input type="text"/>
FREQ. FLYER#	<input type="text"/>	AIRLINE	<input type="text"/>
STORE		CLEAR	

FIG.3

4/15

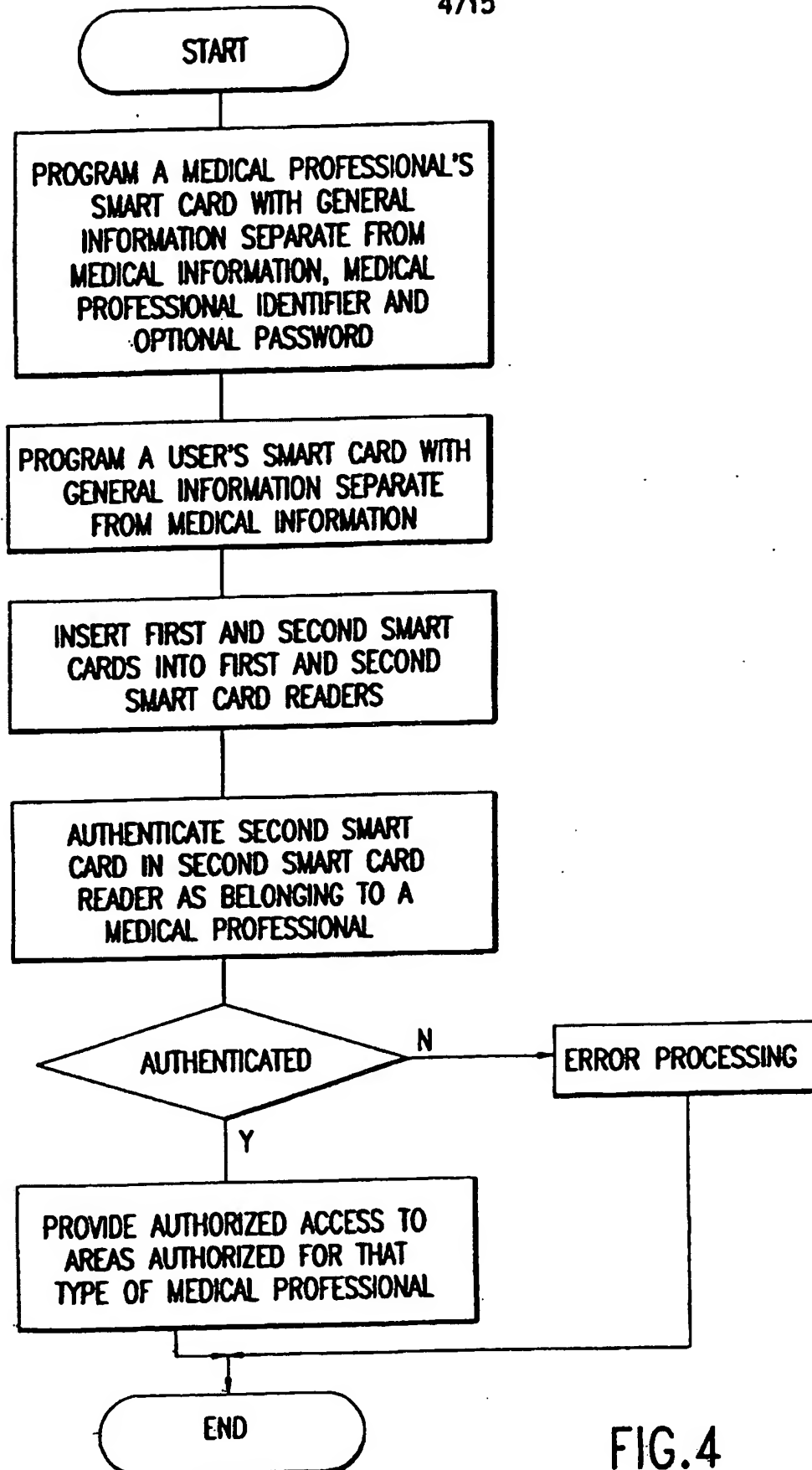


FIG.4

5/15

MEDICAL INFORMATION		7/10/95 14828.0 Kb 00.32	
CARD EXPIRATION DATE			
DATE ISSUED PERSONAL INFORMATION DATE FAMILY NAME ADDRESS CITY, STATE BIRTH DATE SOCIAL SECURITY NO. COUNTRY OF CITIZENSHIP MAILING ADDRESS		07.10.1995 FIRST NAME & INITIAL PHONE # ZIP CODE AGE ID# (PASSPORT #) EMERGENCY CONTACT SEX 1995	
FATHER'S NAME MOTHER'S NAME DESIGNEE PHONE NO.		DURABLE POWER OF ATTORNEY HEALTH CARE SURROGATE LIVING WILL	
BLOOD TYPE MEDICAL ALERT		ALLERGIES	
DOCTOR'S NAME PHONE# WITH COUNTRY CODE FAX# WITH COUNTRY CODE LANGUAGE MEDICAL INSURANCE CO. POLICY NUMBER EMERGENCY CONTACT PHONE INNOCULATIONS		UNDER CARE FOR MEDICATIONS	
STORE		PRINT MEDICAL INFORMATION	
PRINT PERSONAL INFORMATION		PRINT PERSONAL INFORMATION	

FIG. 5

6/15

AREA	PIN	RIGHTS FOR THIS AREA
1	0	R
2	1234	R W C
3	1234	R W C D
3	5678	R C D
3	0911	R
4	1234	R W C
4	0911	R

FIG.6A

7/15

PIN	RIGHTS FOR THIS AREA
0	R
1234	R W C
1234	R W C D
5678	R C D
0911	R

FIG.6B

8/15

PIN	RIGHTS FOR ALL AREAS					
0	R					
1234	R	RWC	RWCD	RWC		
5678	R		RCD			
0911	R		R	R		

FIG. 6C

9/15

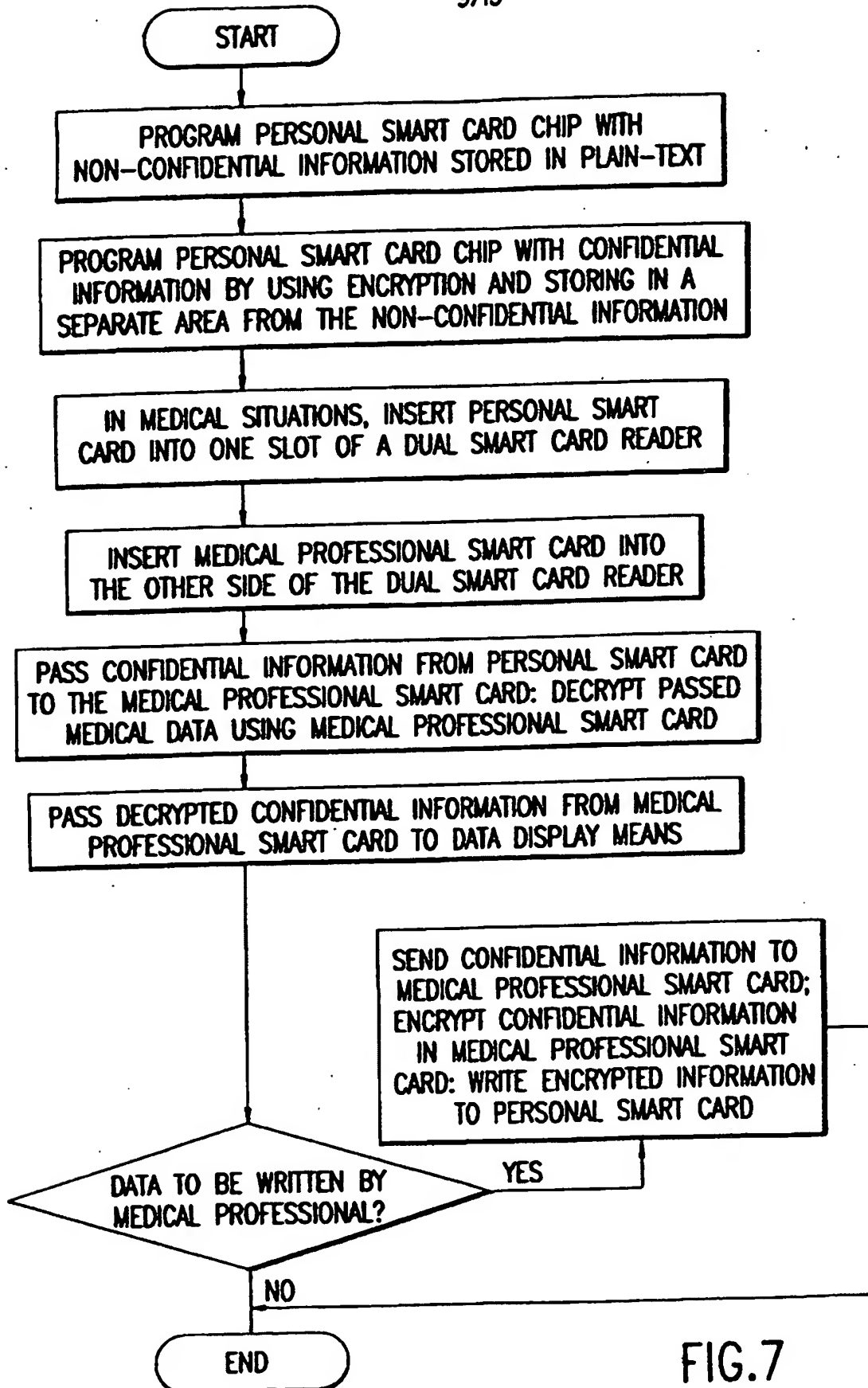


FIG.7

10/15

IMMIGRATION INFORMATION

7/10/95 14840.0 kB 00:31

PERSONALITIES

FAMILY NAME

FIRST NAME [MIDDLE INITIAL]

ADDRESS

CITY/ZIP CODE

COUNTRY OF CITIZENSHIP

COUNTRY WHERE YOU LIVE

PASSPORT # :

BIRTH DATE

SEX

AIRLINE/FLIGHT #

DEPARTURE AIRPORT

ADDRESS IN USA

STREET

CITY

NUMBER

STATE

INFORMATION FOR IMMIGRATION

DATE OF ENTRY 07.10.1995

DATE OF DEPARTURE

PRINT

FIG.8

11/15

52

<div> <div></div> <div>REGISTER OF ARRIVAL</div> <div>7/10/95 14837.0 Kb 00:31</div> </div>				
HOTEL/MOTEL	HONKY TONK		ROOM NO	<div></div>
SURNAME				
FIRST NAME				
PLACE OF BIRTH				
COUNTRY OF RESIDENCE	DATE OF BIRTH			
PROFESSION				
FULL HOME ADDRESS				
ACCOMPANIED BY	<input type="checkbox"/> WIFE/HUSBAND/CHILDREN	NUMBER OF MEMBERS IN PARTY <div></div>		
MODE OF TRANSPORT	<input type="radio"/> PUBLIC <input checked="" type="radio"/> PRIVATE			
DATE OF ARRIVAL	07.10.1995	DATE OF DEPARTURE	<div></div>	
REPRESENTING COMPANY NAME	<div></div>			
PAYMENT TYPE	<div></div>	AMOUNT	<div></div>	
PLATE NO	<div></div>	MODEL/TYPE	<div></div>	
TYPE OF DOCUMENT	PASSPORT	NO	<div></div>	
<div>PRINT</div>				

12/15

56

CAR RENTAL REGISTRATION		7/10/95	14832.0 Kb	00:33
RENTAL STATION NOBRAKE CAR REN		DATE	07.10.1995	
CONTRACT NO.				
CAR TYPE		PLATE NO		
AGREED RETURN STATION		TRUE RETURN STATION		
AGR RETURN DATE		PHONE NO.		
FAMILY NAME				
FIRST NAME & INITIAL				
FULL HOME ADDRESS				
PROFESSION		COUNTRY OF RESIDENCE		
DATE OF BIRTH		PLACE OF BIRTH		
PASSPORT NO.		DRIVERS LICENSE NO.		
CONTACT ADDRESS				
PERSONAL NO. IN		PERSONAL NO. OUT		
PAYMENT TYPE		RENTAL RATE		
<div>PRINT</div>				

13/15

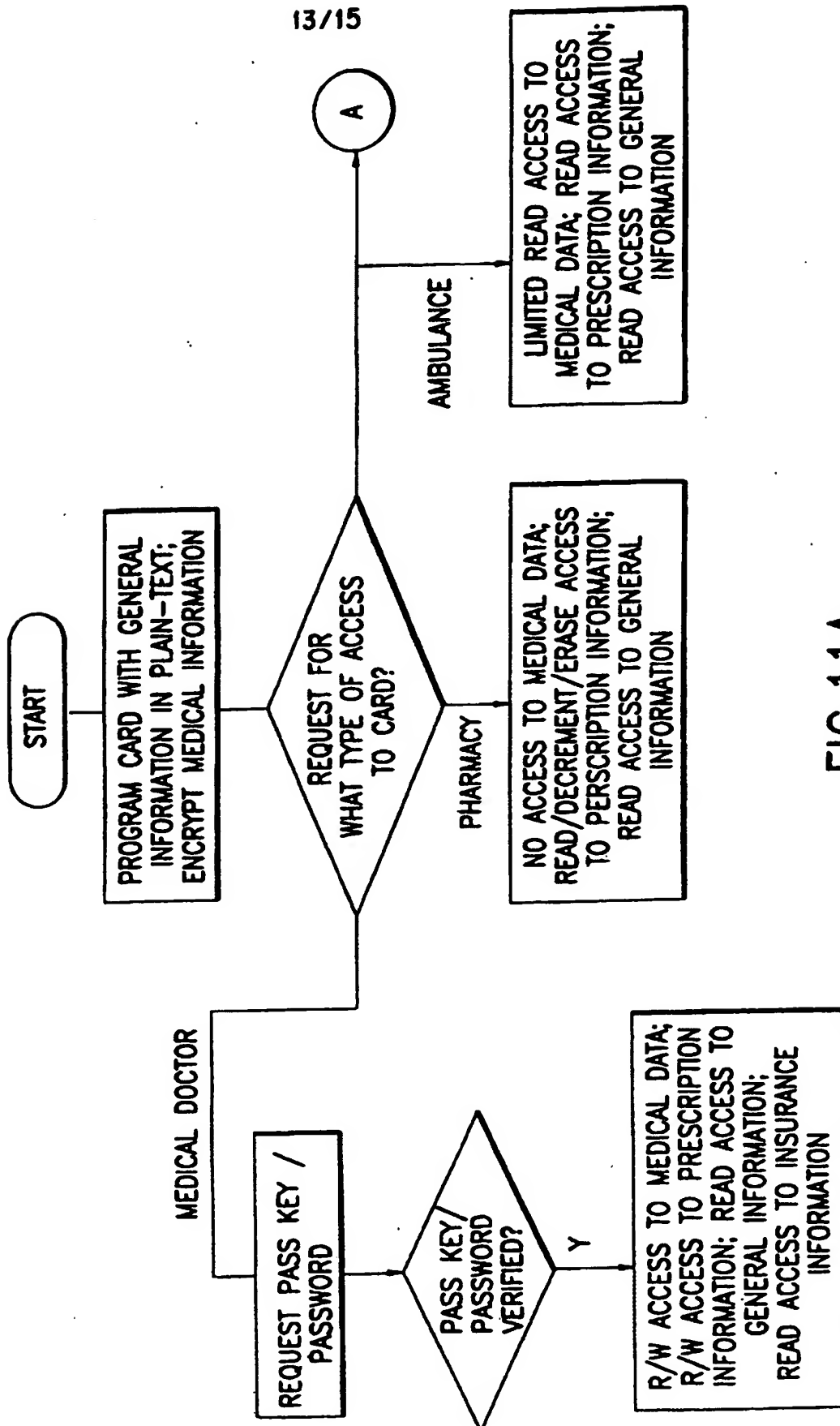


FIG. 11A

14/15

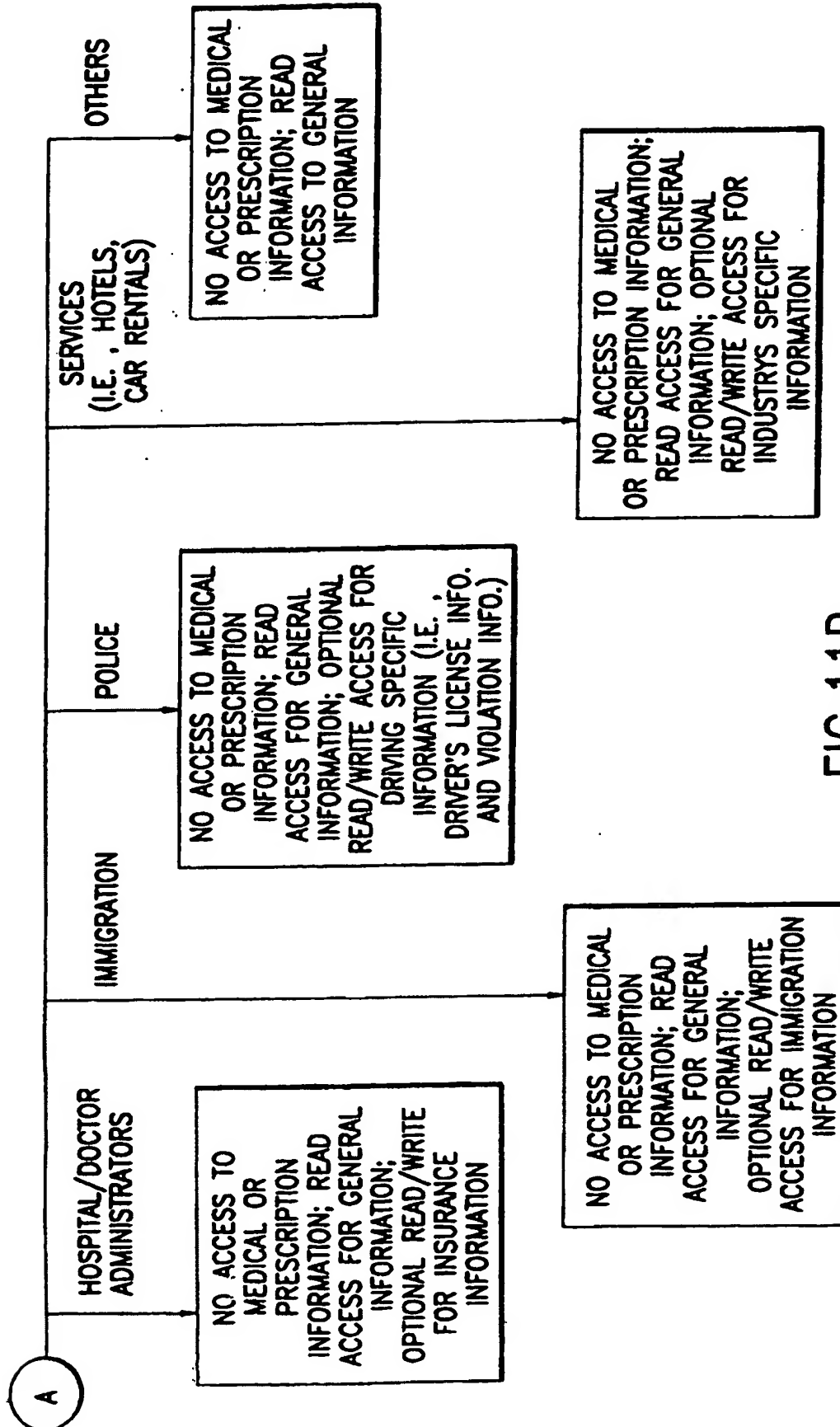


FIG.11B

15/15

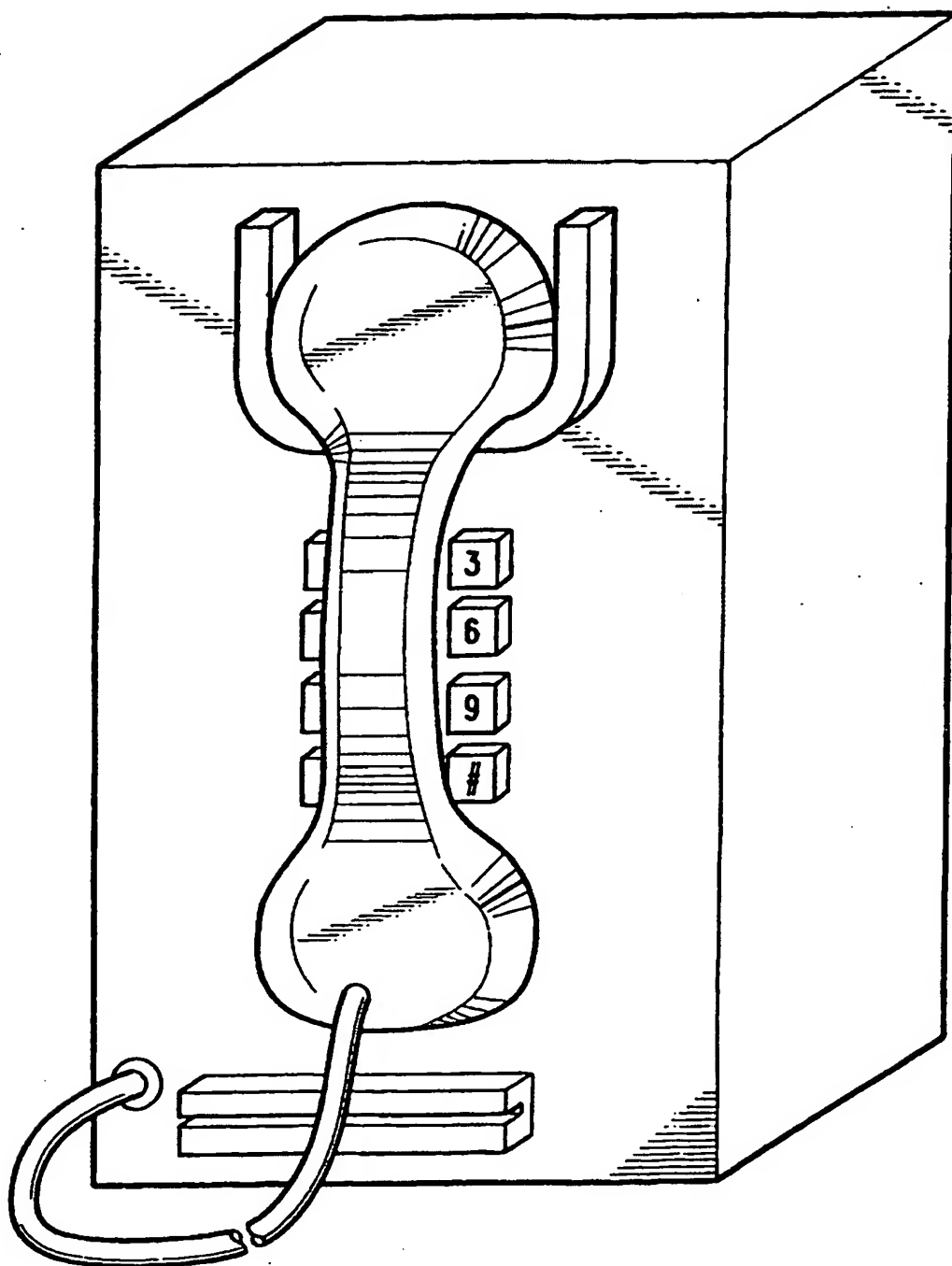


FIG. 12